

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, John T. Dallam, a Special Agent with the United States Secret Service (USSS), being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. This Affidavit is submitted in support of an application for search warrants for the following:

2. Electronic devices used in furtherance of the fraud scheme (together the “**TARGET ELECTRONIC DEVICES**”), as more fully described in Attachment A hereto, which devices are to be searched for evidence, fruits and instrumentalities of violations of 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft) (the “**TARGET OFFENSES**”), as described more fully in Attachment B hereto.

3. This affidavit is made in support of applications for search warrants under Fed. R. Crim. P. 41 and 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A).

4. I am an “investigative or law enforcement officer of the United States” within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18.

5. I am a Special Agent with the United States Secret Service (USSS) and have been since June 2019. During my employment as a United States Secret Service Special Agent, I have been assigned to the Baltimore Field Office where I investigate financial crimes to include access device fraud, bank fraud, identity theft, counterfeit currency, cyber-crimes and protective intelligence. I am a graduate of the Federal Law Enforcement Training Center Criminal Investigator Training Program in Glynco, Georgia. Prior to joining the Secret Service as a Special Agent, I was a Police Officer with the Delmar Police Department in the states of Maryland and Delaware for eight years. I worked as a detective with the State of Delaware Division of Alcohol and Tobacco Enforcement for 5 years where I was assigned to the U.S.

Marshal's First State Fugitive Task Force. I have a bachelor's degree in criminal justice from Wilmington University located in Delaware. I have received training and have extensive experience in interviews, interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, communications platforms, computer networks, network intrusions and various other criminal investigative procedures. I have investigated numerous cases involving financial crimes, protective intelligence, and cyber related crimes.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

7. On 10/07/2020, USSS SA John Dallam was contacted by SA Marjorie Coyne, an investigator with the National Insurance Crime Bureau (NCIB), in reference to a fraud investigation involving a subject identified as Jose Miguel TAPIA. SA Coyne was familiar with TAPIA from prior local and federal prosecutions from when she was a Detective for the Baltimore County Police Department. As a result of the local and federal prosecutions TAPIA was convicted of committing fraudulent activity involving stolen identities as well as stolen bank account information belonging to various businesses. During the investigation into that prior criminal activity, numerous cellular devices had been recovered and examined and it had been determined that TAPIA had been utilizing cellular phones to conduct his activity as opposed to utilizing a computer.

8. Based on SA Coyne's new investigation, during the months of March, 2020 through August, 2021, TAPIA had taken individuals' identity information and created synthetic identities depicting his picture or the picture of his associate(s). In conjunction with the synthetic identities, TAPIA created checks using legitimate routing and account numbers from a law firm and different businesses located in the Baltimore, MD area. Using both the forged checks and synthetic identities, TAPIA purchased various vehicles in the state of Maryland. TAPIA or his associate would conduct the purchase

by going directly into an automobile dealership and using the synthetic identity in conjunction with a forged check to complete the sale of a vehicle or they would communicate with the dealership through the internet, by email and/or by text message in order to complete the deal utilizing a synthetic identity and forged check to finalize the transaction. The dealerships involved would process the payment and release the vehicle to TAPIA, an associate or a transport carrier. In many instances, the dealerships did not discover that the check was fraudulent until several days after the purchase. The victim dealerships had no way to contact TAPIA or recover the vehicles because they were purchased using false information.

9. The checks that TAPIA created contained the name of Integrity Property Services LLC. Further investigation revealed that Integrity Property Services LLC was a business in the state of Maryland registered to TAPIA, 200 Bryan's Way, Reisterstown, MD 21136. The address of 200 Bryan's Way, Reisterstown, MD is also TAPIA's listed primary residence with Maryland Department of Public Safety and Correctional Services Division of Probation and Parole. This address is the primary address that TAPIA used from 2013- 2021. A real property data check for the State of Maryland revealed that the property located at 200 Bryan's Way Reisterstown, MD was sold on 02/12/2020. To date, TAPIA is still using 200 Bryan's Way Reisterstown, MD as his primary address. There is no new information as to the current residence of TAPIA. Through the course of the investigation, over 22 different telephone numbers were found to have been associated to communication conducted between the individuals purchasing or attempting to purchase the various vehicles identified throughout this investigation.

10. On August 24, 2021, at 1945 hours, the Maryland State Police (MSP) Prince Frederick Barrack responded to Winegardner GMC dealership, located at 935 North Solomons Island Road, Prince Frederick, MD in reference to individuals attempting to purchase a vehicle using a fraudulent name. Upon arrival, MSP made contact with the owner identified as Thomas Winegardner. Winegardner informed MSP Troopers that a subject used a name with the initials "NSR" (B/M. DOB:**/**/1962) in an attempt to purchase a 2021 GMC Sierra Denali 1500, valued at \$69,000. NSR provided the dealership with the following documents via email: driver's license, Social Security card and insurance information. The dealership checked the documents to confirm their legitimacy and the query revealed that the driver's

license was invalid. While the query was being conducted, NSR told the dealership that he would be coming to the dealership to pick up the vehicle at approximately 2030 hours.

11. MSP Troopers received information from the dealership that subject NSR was observed being dropped off by a white Lexus with Maryland registration 79436CJ, and that the Lexus was currently parked at the gas pumps at the Exxon station next to the dealership. MSP Troopers made contact with the individual and conducted a field interview. During the field interview, MSP Troopers discovered the real identity of "NSR" to in fact be Deonte Jermele WILLIS-DICKENS (DOB: **/**/1998). Troopers placed WILLIS-DICKENS under arrest for "fraud and providing a false name". A search incident to arrest revealed \$1,480 in genuine U.S. currency on WILLIS-DICKENS' person. When asked about the currency, WILLIS-DICKENS stated he was given the currency to use towards the purchase of the vehicle.

12. Winegardner provided MSP Troopers with the documents that WILLIS-DICKENS provided while attempting to purchase the vehicle. One of the documents provided was a Maryland driver's license bearing the name with the initials "NSR" (DOB: **/**/1962), 3 Maybin Circle, Owings Mills, MD 21117. The driver's license that WILLIS-DICKENS provided pictured a black male. However, database checks for NSR revealed NSR is a white male with the same date of birth used on the fraudulent driver's license (DOB: **/**/1962) but with a different driver's license soundex number.

13. After placing WILLIS-DICKENS under arrest, MSP Troopers responded to the Exxon station located next to the dealership to make contact with the driver of the white Lexus that dropped off WILLIS-DICKENS. MSP Troopers identified the driver of the white Lexus as Jose Miguel TAPIA (B/M, DOB: **/**/1986). During the course of the on-scene investigation, MSP Troopers detected the odor of burnt marijuana emitting from the vehicle, which led to a probable cause search of the vehicle. The search revealed the following: (6) cellular I-Phones and additional marijuana which was determined to belong to TAPIA. MSP Troopers conducted a warrant check of TAPIA which revealed an open warrant through Baltimore City Police Department for failing to appear for narcotics charges. TAPIA was placed under arrest and transported back to the Calvert County, Maryland Detention Center for processing. At

this time a secondary custodial search was conducted of TAPIA's person which revealed additional narcotics. All contraband and phones were seized pending further investigation.

14. Through their investigation, Troopers discovered the driver's license that Willis-Dickens provided to the dealership contained an address of 3 Maybin Circle, Owings Mills, MD 21117. Maryland Motor Vehicle Administration (MVA) records indicated an address change for Jose TAPIA dated 08/06/2020 showing 3 Maybin Circle, Owings Mills, MD 21117 as TAPIA's address.

15. MSP charged WILLIS-DICKENS with the various state fraud and identity theft charges related to the attempted purchase of the vehicle in the identity of NSR..

16. MSP charged J. TAPIA with possession of a controlled dangerous substance and accessory after the fact in relation to the felony involving fraud.

17. Jose Miquel TAPIA is currently incarcerated in the Baltimore City Detention Center on charges related to the warrant out of Baltimore City Maryland, for which he was arrested. Deonte Willis-Dickens has an active warrant for failure to appear on the charges listed above.

18. On March 25, 2022, USSS SA John Dallam was contacted by the Maryland State Police (MSP), Prince Frederick Barrack, Calvert County, Maryland in reference to (6) cellular phones that were recovered from Jose Miguel TAPIA as the result of their criminal investigation. MSP advised that their criminal case against TAPIA had been adjudicated and the phones could be released to the United States Secret Service for forensic analysis in reference to their current fraud investigation involving Jose Miguel TAPIA.

TECHNICAL TERMS

19. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling

voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

20. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

21. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

22. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current

time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

23. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical

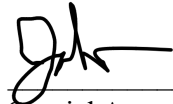
intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

27. Based upon my training and experience and the foregoing facts, I submit that there is probable cause to believe that the (6) cellular phones belonging to JOSE MIGUEL TAPIA are currently involved in an ongoing identity fraud and bank fraud case and the "Devices to be Searched" contain evidence, fruits, and instrumentalities of the aforementioned fraudulent activities, as described in Attachment B.

CONCLUSION

28. Based on the foregoing information, your Affiant asserts that there is probable cause to believe that evidence relating to the **TARGET OFFENSES** will be found in the **TARGET ELECTRONIC DEVICES** currently being held by the Maryland State Police, Prince Frederick Barrack located at 210 Main St, Prince Frederick, Maryland 20678.

Respectfully submitted,

 04/12/2022
Special Agent John T. Dallam
UNITED STATES SECRET SERVICE

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 14th of April 2022.


THE HONORABLE MATTHEW J. MADDOX
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Description of Items to be Searched (The Subject Electronic Devices)

1. Blue Apple I-Phone cell phone with Red and White cell phone case
2. Gold Apple I-Phone cell phone with Black case
3. Dark Blue Apple I-Phone cell phone with no case
4. Red Apple I-Phone cell phone with Red case
5. Blue Apple I-Phone cell phone with Red and White case
6. Grey Apple I-Phone cell phone with Brown case

ATTACHMENT B - THE THINGS TO BE SEARCHED

The items described in Attachment A may be searched for the following things, which may be seized:

All records, documents, messages, correspondence, data, and materials that may constitute fruits or instrumentalities of, or contain evidence related to, 18 U.S.C. § 1344 (Bank Fraud and Related Activity), and 18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft), including, but not limited to, the following:

1. Documents and records containing bank account numbers, debit and/or credit card numbers, personal identification numbers, and other access devices;
2. Any and all documents containing personal identifying information of potential victims, including, but not limited to, bank account statements and credit card statements;
3. Identification records and documents, such as birth certificates, SSN cards, driver's licenses, voter registration cards, passports, and applications for such identification documents;
4. Messages, Text messages, SMS messages, correspondence, and personal records bearing any individual names, such as mail items addressed to or from any named individual;
5. Financial documents, such as bank account records and statements, IRS forms, and state tax records;
6. Any contact logs, address books, telephone books, notes reflecting telephone numbers, photographs, phone or email directories that may identify the names of participants in the fraud scheme described in the Affidavit including but not limited to any and all documents that refer or relate to JOSE MIGUEL TAPIA, or that may identify other co-conspirators in the scheme.

As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials created, modified, or stored in electronic or digital form, and by whatever means they may have been created and/or stored. This includes any photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes

things in the form of computer hardware, software, documentation, passwords, and/or data security devices.

The search procedure of the electronic data contained in computer operating software or memory devices may include the following techniques, which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:

- a. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- c. “scanning” storage areas to discover and possibly recover recently deleted files;
- d. “scanning” storage areas for deliberately hidden files; or
- e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files, or storage areas do not reveal evidence of identity theft, or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of items that are identified with particularity in the warrant while minimizing the review of any information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.